PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-261788
(43)Date of publication of application : 24.09.1999

(51)Int.Cl. H04N 1/32
G09C 1/00
H04L 9/32
H04L 9/36
// H04N 1/44

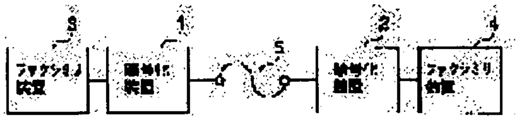
(21)Application number : 10-059208
(22)Date of filing : 11.03.1998

(71)Applicant : ALPS ELECTRIC CO LTD
(72)Inventor : KANBAYASHI SHIZUO

(54) ENCRYPTION DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To allow a device to send/receive a confidential document without making notice of transmission of a confidential document in advance and to reduce the communication cost by compressing data while keeping secrecy of contents through encryption.

SOLUTION: An encryption device 1 is provided between a transmitter side communication terminal 3 and a communication network 5 and an encryption device 2 is provided between a receiver side communication terminal 4 and the communication network 5. A document and a password entered from the communication terminal 3 at the transmitter side are compressed and the compressed document and password are sent to the receiver side via the communication network 5, the receiver side decompresses the compressed document and password received via the communication network 5 and outputs the result to the communication terminal 4 at the receiver side.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] Encryption equipment characterized by it being prepared between the communication terminal of a transmitting side, and a communication network, and between the communication terminal of a receiving side, and a communication network, compressing the document and the password which were entered from said communication terminal in the transmitting side, transmitting said compressed document and compressed password to a receiving side through said communication network, thawing said document and password which were received through said communication network in the receiving side, and which were compressed, and making it output to the communication terminal of said receiving side.
[Claim 2] Encryption equipment according to claim 1 characterized by enciphering said compressed document and compressed password in a transmitting side, decoding said document and password which were compressed and enciphered by the receiving side, and making it output to the communication terminal of a receiving side.
[Claim 3] Encryption equipment according to claim 2 characterized by thawing and decoding said document which was received through said communication network, and which was compressed and enciphered in a receiving side, and making it output the specific region of said document thawed and decoded, and said document which was received through said communication network, and which was compressed and enciphered to said communication terminal of a receiving side.
[Claim 4] Encryption equipment according to claim 3 characterized by making it output said document thawed and decoded with the password entered into said communication terminal of a receiving side in a receiving side when said document and password which were compressed and enciphered are received.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] It connects between communication terminals, such as facsimile apparatus, and the telephone line, and this invention relates to the encryption equipment which enables transmission and reception of a confidential document.
[0002]
[Description of the Prior Art] Drawing 3 explains the transceiver approach of the confidential document using the conventional facsimile apparatus. In drawing 3 , since the transceiver approach (for example, how to decide a password) of a confidential document changes with each manufacturers of facsimile apparatus in order to transmit and receive a confidential document, the facsimile apparatus 31 and 32 of the same manufacturer having the confidential function of the same approach have been formed in the transmitting side and the receiving side. Moreover, both the facsimile apparatus 31 and 32 are connected to the dial-up line 33. Here, when a confidential document is received, the check lamp which tells the reception is formed in the facsimile apparatus 31 and 32 with the confidential function connected to the transmitting side and the receiving side.
[0003] And the password is beforehand decided between a transmitting person and a recipient's both sides, and when transmitting a confidential document, a transmitting person starts transmission of a confidential document, after he notifies a recipient of the purport which transmits a confidential document by telephone contact etc. In that case, a transmitting person inputs the telephone number, password, and confidential document of the phase hand who transmits into the facsimile apparatus 31 of a transmitting side first. Then, facsimile apparatus 31 compresses a confidential document among the entered password and a confidential document (for example, MH method and MR method). And the password and the compressed confidential document inputted with the facsimile apparatus 31 of a transmitting side are transmitted to the facsimile apparatus 32 of a receiving side through a dial-up line 33. On the other hand, the facsimile apparatus 32 of the receiving side which received the confidential document judges that the transmitted document is a confidential document, and makes a check lamp turn on by receiving a password first. In this phase, the printout is not carried out for the confidential document. And a recipient checks lighting of a check lamp and enters a password into the facsimile apparatus 32 of a receiving side. If this password and the password entered with the facsimile apparatus 31 of a transmitting side are in agreement, facsimile apparatus 32 will thaw the compressed confidential document, and will output a confidential document.
[0004]
[Problem(s) to be Solved by the Invention] By the way, although the recipient was able to check whether the received document was a confidential document since the check lamp which tells reception of a confidential document was formed, there was no means of 32 facsimile apparatus with a confidential function of a receiving side to check whether it is the confidential document with which the confidential document was addressed and sent to whom of a receiving side. Therefore, since the transmitting person had transmitted the confidential document after telling the recipient of the other party transmitting a confidential document by the telephone, facsimile, etc. beforehand, only the part which tells transmitting a confidential document required communication link cost, and he was also waste of energy. moreover, the received confidential document -- whom -- since it was not able to check whether it was the confidential document sent to addressing, derangement had been produced when there were other recipients who will

prepare it if I will receive a confidential document to the other party from a different partner. Furthermore, since the data to transmit became large when a lot of documents were transmitted, the communication link took time amount and communication link cost had started. Moreover, since the confidential document was sent using the telephone line etc., with the condition of having compressed, there was a danger that the contents of the confidential document would be stolen by the third person.

[0005] This invention solves these problems, and it is compressing further the data compressed with facsimile apparatus, and the purpose shortens communication link time amount, and is to press down traffic. Moreover, the purpose of this invention is by making it a confidential document reach a recipient, holding the secret of the contents by enciphering a confidential document, and putting in the password with which the recipient was decided in that case, to enable it to make a confidential document output, without notifying the purport to which a transmitting person sends a confidential document beforehand.

[0006]

[Means for Solving the Problem] In order to solve the above-mentioned problem, the encryption equipment of this invention It is prepared between the communication terminal of a transmitting side, and a communication network, and between the communication terminal of a receiving side, and a communication network. The document and password which were entered from the communication terminal were compressed, and the document and password which were compressed were transmitted to the receiving side through the communication network, and the document and password which were received through the communication network and which were compressed are thawed, and it was made to output to the communication terminal of a receiving side at a receiving side in a transmitting side.

[0007] Moreover, the encryption equipment of this invention decodes the document which enciphered the compressed document and the compressed password, and was compressed and enciphered by the receiving side, and it was made to output it to the communication terminal of a receiving side in a transmitting side.

[0008] Moreover, it was made for the encryption equipment of this invention to output the specific region of the document which thawed and decoded, and was thawed and decoded in the document which was received through the communication network, and which was compressed and enciphered, and the document which was received through the communication network and which was compressed and enciphered to the communication terminal of a receiving side in a receiving side.

[0009] Moreover, when the document and password which were compressed and enciphered were received, it was made for the encryption equipment of this invention to output the document decoded as boil the password entered into the communication terminal of a receiving side in a receiving side.

[0010]

[Embodiment of the Invention] The outline of the transceiver approach of the confidential document using the encryption equipment of this invention is explained according to drawing 1 . In drawing 1 , both the encryption equipments 1 and 2 of this invention are equipped with the same configuration and the same function, it is used for a transmitting side and a receiving side, the facsimile apparatus 3 which is the communication terminal of a transmitting side is connected to the encryption equipment 1 of a transmitting side, and, on the other hand, the facsimile apparatus 4 which is the communication terminal of a receiving side is connected to the encryption equipment 2 of a receiving side. And the encryption equipment 1 of a transmitting side and the encryption equipment 2 of a receiving side are connected to the dial-up line 5 which is a communication network, it is compressed and enciphered with the encryption equipment 1 of a transmitting side, and the confidential document inputted into the facsimile apparatus 3 of a transmitting side is sent out to a dial-up line 5. On the other hand, with encryption equipment 2, the confidential document (condition enciphered and compressed) inputted through the dial-up line 5 is thawed and decoded, and is outputted to the facsimile apparatus 4 of a receiving side.

[0011] Next, drawing 2 explains the encryption equipments 1 and 2 of this invention. Here, both sides have the transmitting section 6 and a receive section 7, and the encryption equipments 1 and 2 shown in drawing 1 are constituted so that the confidential document of each other can be transmitted and received. In addition, drawing 2 shows only the receive section 7 of the encryption equipment 2 of the receiving side of drawing 1 only for the transmitting section 6 of the encryption equipment 1 of the transmitting side of drawing 1 again. First, the transmitting section 6 of encryption equipment 1 consists of the reception-control section 8, the memory section 9, the password Management Department 10, the cipher-processing section 11, and the transmitting-side communications control section 12. Moreover, the receive section 7 of encryption equipment 2 consists of the receiving-side communications control section 13, the memory section 14, the decode processing section 15, the password Management Department 16, and the transmit/receive control section 17. In addition, the encryption equipments 1 and 2 have the transceiver function of the usual document, and the transceiver function of a confidential document, and have further the circuit changing switch (not shown) which changes both functions. And it changes to one of functional conditions with a circuit changing switch. Moreover, a function is changed from the facsimile apparatus connected also by the approach of inputting an instruction of a functional change without changing the function by the circuit changing switch. Here, when usually using it, a circuit changing switch is changed, it is set as the function with much operating frequency, and changes with a circuit changing switch if needed, or an instruction of a functional change is inputted from facsimile apparatus, and a function is changed.

[0012] Next, the transmitting approach of a confidential document is explained. Here, the password is beforehand decided between the transmitting person and the recipient, and a transmitting person indicates the information (henceforth transmitting person information) which specifies a recipient's address and transmitting person as the specific region (for example, part of 8cm of upper parts of the first page) of a confidential document. And the password which decided encryption equipment 1 beforehand to be an instruction of the change for making it operate by the confidential function, a phase hand's telephone number, and a confidential document are inputted into the facsimile apparatus 3 of a transmitting side. Then, facsimile apparatus 3 compresses a confidential document among the inputted information. (For example, MH method and MR method.) And the compressed confidential document is hereafter called confidential data, the facsimile apparatus 3 of a transmitting side transmits the password which decided the encryption equipment 1 of a transmitting side beforehand to be the instruction for making it operate by the confidential function, a phase hand's telephone number, and confidential data to the encryption equipment 1 of a transmitting side. Here, encryption equipment 1 serves as confidential functional actuation, and will be in the condition of transmitting a confidential document. And encryption equipment 1 reads the confidential data and the password which were received from facsimile apparatus 3 in the reception-control section 8 of the transmitting section 6, and sends them to the memory section 9.

[0013] Next, a password is changed into the instruction for making the encryption equipment 2 of a receiving side process the transmitted document by the confidential function by the password Management Department 10 among the confidential data and the passwords which were sent in the memory section 9 (henceforth header-ization). Next, confidential data and the header-ized password are enciphered and compressed by the cipher-processing section 11 (the confidential data enciphered and compressed and the header-ized password are hereafter put in block, and it is called transmit data). And transmit data is transmitted to the encryption equipment 2 of a receiving side by the transmitting-side communications control section 12 through a dial-up line 5. Thus, since the document compressed with facsimile apparatus 3 was compressed further and it has transmitted, a lot of documents can be transmitted in a short time. Moreover, since the contents cannot be known even if a confidential document is stolen by the third person in the middle of transmission, since the document was enciphered and it has transmitted with encryption equipment 1, the nondisclosure of the contents of a document which transmits is made possible.

[0014] Next, the reception approach of a confidential document is explained. First, the transmit data transmitted through the dial-up line 5 is read in the receiving-side communications control section 13 of the encryption equipment 2 of a receiving side, and is sent to the memory section 14. And the transmit data sent to the memory section 14 is returned to confidential data before being thawed, and decoded and transmitted by the decode processing section 15, and the header-ized password, and is again sent to the memory section 14. Here, in the memory section 14, the transmit data in the condition of having been transmitted from the encryption equipment 1 of a transmitting side (what compressed and enciphered confidential data and the header-ized password), the password in the condition of having been decoded and thawed, and confidential data are saved. Next, as for the header-ized password which was saved in the memory section 14, a password is read by the password Management Department 16.

[0015] And the transmit data (what compressed and enciphered confidential data and the header-ized password) saved in the memory section 14, and the transmitting person information on the confidential document thawed and decoded are transmitted to the facsimile apparatus 4 of a receiving side by the transmit/receive control section 17. And as for the transmitting person information and the transmit data which were transmitted from the transmit/receive control section 17, the first printout is made by the facsimile apparatus 4 of a receiving side. Here, since the transmit data printed with transmitting person information is transmit data in the condition that the encryption equipment 2 of a receiving side received (what compressed and enciphered confidential data and the header-ized password), the first printout is made while the confidential document had been enciphered.

[0016] In addition, if this is all printed when the transmit data in the condition that the encryption equipment 2 of a receiving side received (what compressed and enciphered confidential data and the header-ized password) is extensive, a facsimile form will be used vainly. Then, it enables it to check that the document received in the transmit data in the condition that the encryption equipment 2 of a receiving side received transmitted to the facsimile apparatus 4 of a receiving side from the encryption equipment 2 of a receiving side because some transmit data (for example, 2cm) print transmitting person information under the printed part is a confidential document. In addition, it has set up beforehand so that it may print on the space with same transmitting person information and transmit data in the condition of having received. Therefore, a recipient can check a transmitting person and the destination by one transmission by filling in the information which specifies a recipient's address and transmitting person as the specific region of a confidential document. Furthermore, since it is outputted in the condition [that some transmit data are enciphered], even if a third person sees, a transmitting person can transmit a confidential document, holding the secret of the contents, and a recipient can check easily that the received document is a confidential document.

[0017] Next, the second printout approach which outputs all the received confidential documents is explained. First, the transmit data and the decoded confidential document are saved in the memory section 14 in the receive section 7 of encryption equipment 2. Here, a recipient enters into the facsimile apparatus 4 of a receiving side the password decided beforehand. Then, the transmit/receive control section 17 reads the password entered into facsimile apparatus 4, and transmits to the memory section 14. And the password Management Department 10 collates whether the password in the condition of having been decoded and thawed saved in the memory section 14, and the password entered into the facsimile apparatus 4 of a receiving side are in agreement. Here, if the password in the condition of having been decoded and thawed, and the password entered into the facsimile apparatus 4 of a receiving side are in agreement and it will be checked by the password Management Department 10, the transmit/receive control section 17 will transmit the confidential document which was saved in the memory section 14 and which was decoded and thawed to the facsimile apparatus 4 of a receiving side. And as for the confidential document decoded and thawed, the second printout is made by the facsimile apparatus 4 of a receiving side. Thus, only the recipient is being able to carry out the printout of the confidential document by enabling it to carry out the printout of the confidential document in entering the password which the recipient decided beforehand.

[0018]

[Effect of the Invention] As mentioned above, the encryption equipment of this invention is formed between the communication terminal of a transmitting side, and a communication network, and between the communication terminal of a receiving side, and a communication network. Compress the document and password which were entered from the communication terminal in the transmitting side, and the document and password which were compressed are transmitted to a receiving side through a communication network. The document and password which were received through the communication network in the receiving side and which were compressed are thawed, and by having made it output to the communication terminal of a receiving side, since communication link time amount is shortened in order to compress further the document compressed with facsimile apparatus, traffic is reducible.

[0019] moreover, the thing the encryption equipment of this invention enciphers the document and password which were compressed in the transmitting side, compresses them by the receiving side, decode the enciphered document, and it was made output to the communication terminal of a receiving side -- it is -- transmission -- on the way -- it comes out and a confidential document is stolen for a third person -- also having -- since the confidential document is enciphered and the contents cannot be known, the nondisclosure of the contents of a document which transmits is made possible.

[0020] Moreover, the specific region of the document with which it thawed and decoded, and the encryption equipment of this invention was thawed and decoded in the receiving side in the document which was received through the communication network, and which was compressed and enciphered, The document which was received through the communication network and which was compressed and enciphered by having made it output to the communication terminal of a receiving side For example, a confidential document can be transmitted and received by indicating the information which a recipient's address and a transmitting person specify to a specific region, without notifying the purport which sends a confidential document beforehand.

[0021] Moreover, when the document and password which were compressed and enciphered in the receiving side are received, the encryption equipment of this invention is having made it output the decoded document with the password entered into the communication terminal of a receiving side, and makes it possible to carry out the printout of the confidential document with which only the recipient who knows the password was thawed and decoded.

[Translation done.]

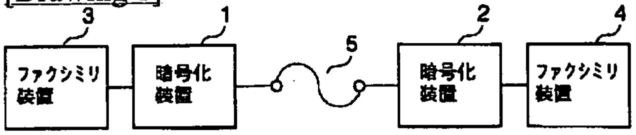
* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

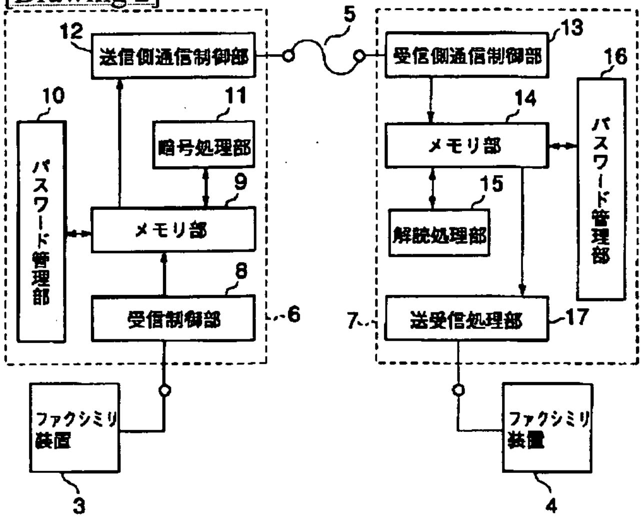
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

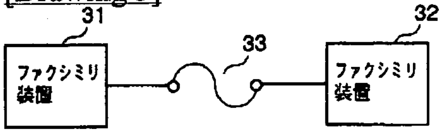
[Drawing 1]



[Drawing 2]



[Drawing 3]



[Translation done.]

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-261788
(43)Date of publication of application : 24.09.1999

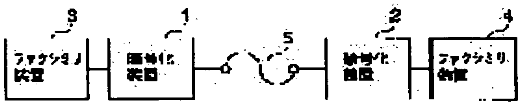
(51)Int.Cl.	H04N 1/32 G09C 1/00 H04L 9/32 H04L 9/36 // H04N 1/44

(21)Application number :	10-059208	(71)Applicant :	ALPS ELECTRIC CO LTD
(22)Date of filing :	11.03.1998	(72)Inventor :	KANBAYASHI SHIZUO

(54) ENCRYPTION DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To allow a device to send/receive a confidential document without making notice of transmission of a confidential document in advance and to reduce the communication cost by compressing data while keeping secrecy of contents through encryption.
SOLUTION: An encryption device 1 is provided between a transmitter side communication terminal 3 and a communication network 5 and an encryption device 2 is provided between a receiver side communication terminal 4 and the communication network 5. A document and a password entered from the communication terminal 3 at the transmitter side are compressed and the compressed document and password are sent to the receiver side via the communication network 5, the receiver side decompresses the compressed document and password received via the communication network 5 and outputs the result to the communication terminal 4 at the receiver side.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

5

(19)日本国特許庁（ＪＰ）

(12) 公開特許公報（A）

(11)特許出願公開番号
特開平11－261788

(43)公開日 平成11年(1999) 9月24日

(51)Int.Cl.⁶	識別記号	F I	
H04N 1/32		H04N 1/32	G
G09C 1/00	640	G09C 1/00	640E
H04L 9/32		H04N 1/44	
9/36		H04L 9/00	673C
// H04N 1/44			685

審査請求 未請求 請求項の数4 OL （全 5 頁）

(21)出願番号 特願平10－59208

(22)出願日 平成10年(1998) 3月11日

(71)出願人 000010098
アルプス電気株式会社
東京都大田区雪谷大塚町1番7号

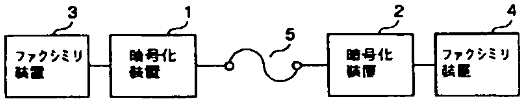
(72)発明者 神林 静夫
東京都大田区雪谷大塚町1番7号 アルプス電気株式会社内

(54)【発明の名称】 暗号化装置

(57)【要約】

【課題】 あらかじめ親展文書を送る旨の通知をすることなく親展文書の送受信をおこなうことができ、暗号化することで内容の秘密を保持しつつ、データの圧縮をすることで通信費を押さえる。

【解決手段】 送信側の通信端末3と通信網5との間及び受信側の通信端末4と通信網5との間に設けられ、送信側では通信端末3から入力された文書とパスワードとを圧縮し、圧縮した文書とパスワードとを通信網5を介して受信側に送信し、受信側では通信網5を介して受信した圧縮した文書とパスワードとを解凍し、受信側の通信端末4に出力するようにした。



【特許請求の範囲】

【請求項１】　送信側の通信端末と通信網との間及び受信側の通信端末と通信網との間に設けられ、送信側では前記通信端末から入力された文書とパスワードとを圧縮し、前記圧縮した文書とパスワードとを前記通信網を介して受信側に送信し、受信側では前記通信網を介して受信した前記圧縮された文書とパスワードとを解凍し、前記受信側の通信端末に出力するようにしたことを特徴とする暗号化装置。

【請求項２】　送信側では前記圧縮した文書とパスワードとを暗号化し、受信側で前記圧縮し、暗号化した文書とパスワードとを解読して受信側の通信端末に出力するようにしたことを特徴とする請求項１記載の暗号化装置。

【請求項３】　受信側において、前記通信網を介して受信した前記圧縮し、暗号化した文書を解凍及び解読し、前記解凍及び解読された文書の特定領域と、前記通信網を介して受信した前記圧縮し、暗号化した文書とを受信側の前記通信端末に出力するようにしたことを特徴とする請求項２記載の暗号化装置。

【請求項４】　受信側において、前記圧縮し暗号化された文書とパスワードとを受信したときに、受信側の前記通信端末に入力されたパスワードによって、前記解凍及び解読した文書を出力するようにしたことを特徴とする請求項３記載の暗号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ファクシミリ装置等の通信端末と電話回線との間に接続されて、親展文書の送受信を可能とする暗号化装置に関する。

【０００２】

【従来の技術】従来のファクシミリ装置を用いた親展文書の送受信方法について、図３によって説明する。図３において、親展文書の送受信を行うためには、ファクシミリ装置の各メーカーによって親展文書の送受信方法（例えば、パスワードの決め方）が異なっているので、同じ方法の親展機能を備えた同一メーカーのファクシミリ装置３１及び３２を送信側及び受信側に設けている。また、両ファクシミリ装置３１及び３２は公衆電話回線３３に接続されている。ここで、送信側及び受信側に接続された親展機能を持つファクシミリ装置３１及び３２には、親展文書を受信したときに、その受信を知らせる確認ランプ等が設けられている。

【０００３】そして、あらかじめ送信者と受取人の双方の間でパスワードを決めておき、送信者は、親展文書を送信するときは、親展文書を送信する旨を電話連絡等によって受取人に通知した後で親展文書の送信を開始する。その場合に、まず送信者は、送信側のファクシミリ装置３１に、送信する相手先の電話番号、パスワード及び親展文書を入力する。すると、ファクシミリ装置３１は、入力されたパスワード及び親展文書のうち、親展文書を圧縮するようになっている（例えば、ＭＨ方式やＭＲ方式）。そして、送信側のファクシミリ装置３１で入力されたパスワード及び圧縮された親展文書は、公衆電話回線３３を通じて受信側のファクシミリ装置３２に送信される。一方、親展文書を受信した受信側のファクシミリ装置３２は、まず、パスワードを受信することによって、送信された文書が親展文書であると判断して、確認ランプを点灯させる。この段階では、親展文書は印字出力はされていない。そして、受取人は、確認ランプの点灯を確認して受信側のファクシミリ装置３２にパスワードを入力する。このパスワードと、送信側のファクシミリ装置３１で入力したパスワードとが一致すると、ファクシミリ装置３２は圧縮された親展文書を解凍し、親展文書を出力するようになっていた。

【０００４】

【発明が解決しようとする課題】ところで、親展機能を持つ受信側のファクシミリ装置３２は、親展文書の受信を知らせる確認ランプ等が設けられているので、受取人は、受信した文書が親展文書であるか否かを確認することは出来たが、その親展文書が受信側の誰に宛てて送られた親展文書であるかを確認する手段はなかった。そのため、送信者は、あらかじめ相手側の受取人に親展文書を送信することを、電話やファクシミリ等で伝えてから親展文書を送信していたため、親展文書を送信することを伝える分だけ、通信コストがかかり、かつ、二度手間でもあった。また、受信した親展文書が誰宛てに送られた親展文書であるかを確認することは出来なかったので、相手側に、異なる相手から親展文書を受信しようと準備している、他の受取人がいる場合は混乱を生じていた。さらに、大量の文書を送信する場合には、送信するデータが大きくなるので、通信に時間がかかり、通信コストがかかっていた。また、電話回線等を用いて親展文書を送るので、圧縮した状態のままでは、第三者に親展文書の内容を盗まれる危険性があった。

【０００５】本発明は、これらの問題を解決するもので、その目的は、ファクシミリ装置で圧縮されたデータを更に圧縮することで、通信時間を短縮させて、通信費を押さえることにある。また、本発明の目的は、送信者があらかじめ親展文書を送る旨の通知をすることなく親展文書が受取人に届くようにし、その際、親展文書を暗号化することで、その内容の秘密を保持し、受取人が決められたパスワードを入れることによって、親展文書を出力させることが出来るようにすることにある。

【０００６】

【課題を解決するための手段】上記問題を解決するために、本発明の暗号化装置は、送信側の通信端末と通信網との間及び受信側の通信端末と通信網との間に設けられ、送信側では通信端末から入力された文書とパスワードとを圧縮し、圧縮された文書とパスワードとを通信網

を介して受信側に送信し、受信側では通信網を介して受信した圧縮された文書とパスワードとを解凍し、受信側の通信端末に出力するようにした。

【０００７】また、本発明の暗号化装置は、送信側では圧縮した文書とパスワードとを暗号化し、受信側で圧縮し、暗号化した文書を解読して受信側の通信端末に出力するようにした。

【０００８】また、本発明の暗号化装置は、受信側において、通信網を介して受信した圧縮し、暗号化した文書を解凍及び解読し、解凍及び解読された文書の特定領域と、通信網を介して受信した圧縮し、暗号化した文書とを受信側の通信端末に出力するようにした。

【０００９】また、本発明の暗号化装置は、受信側において、圧縮し暗号化された文書とパスワードとを受信したときに、受信側の通信端末に入力されたパスワードをによって、解読した文書を出力するようにした。

【００１０】

【発明の実施の形態】本発明の暗号化装置を用いた親展文書の送受信方法の概略を図１に従って説明する。図１において、本発明の暗号化装置１、２は、共に同一の構成及び同一の機能を備え、送信側と受信側とに使用され、送信側の暗号化装置１に送信側の通信端末であるファクシミリ装置３が接続され、一方、受信側の暗号化装置２に受信側の通信端末であるファクシミリ装置４が接続される。そして、送信側の暗号化装置１と受信側の暗号化装置２とが、通信網である公衆電話回線５に接続され、送信側のファクシミリ装置３に入力された親展文書は、送信側の暗号化装置１で圧縮及び暗号化されて、公衆電話回線５に送出される。一方、公衆電話回線５を介して入力された親展文書（暗号化及び圧縮された状態）は、暗号化装置２によって解凍及び解読され、受信側のファクシミリ装置４に出力するようになっている。

【００１１】次に、本発明の暗号化装置１及び２を図２により説明する。ここで、図１に示す暗号化装置１及び２は、双方とも送信部６及び受信部７を備え、互いに親展文書を送受信することが出来るように構成されている。なお、図２では、図１の送信側の暗号化装置１の送信部６のみを、また、図１の受信側の暗号化装置２の受信部７のみを示している。まず、暗号化装置１の送信部６は、受信制御部８、メモリ部９、パスワード管理部１０、暗号処理部１１及び送信側通信制御部１２とから構成されている。また、暗号化装置２の受信部７は、受信側通信制御部１３、メモリ部１４、解読処理部１５、パスワード管理部１６及び送受信制御部１７とから構成されている。なお、暗号化装置１と２とは、通常の文書の送受信機能と親展文書の送受信機能とを有し、さらに、双方の機能を切り替える切替スイッチ（図示せず）を有している。そして、切替スイッチによっていずれかの機能状態に切り替えられるようになっている。また、切替スイッチによる機能の切り替えをしないで、接続されているファクシミリ装置から機能切り替えの命令を入力する方法によっても、機能を切り替えられるようになっている。ここで、通常使用するときは、切替スイッチを切り替え、使用頻度の多い機能に設定しておき、必要に応じて、切替スイッチによって切り替えるか、ファクシミリ装置から機能切り替えの命令を入力して機能を切り替えるようになっている。

【００１２】次に、親展文書の送信方法について説明する。ここで、あらかじめ送信者と受取人との間でパスワードを決めておき、送信者は、親展文書の特定領域（例えば、最初のページの上部８ｃｍの部分）に、受取人の宛名及び送信者を特定する情報（以下、送信者情報という）を記載する。そして、送信側のファクシミリ装置３に、暗号化装置１を親展機能で動作させるための切り替えの命令と、あらかじめ決めたパスワードと、相手先の電話番号と、親展文書とを入力する。すると、ファクシミリ装置３は、入力された情報のうち、親展文書を圧縮するようになっている。（例えば、ＭＨ方式やＭＲ方式。以下、圧縮された親展文書を親展データという）そして、送信側のファクシミリ装置３は、送信側の暗号化装置１を親展機能で動作させるための命令と、あらかじめ決めたパスワードと、相手先の電話番号と、親展データとを送信側の暗号化装置１に送信する。ここで、暗号化装置１は、親展機能動作となり、親展文書を送信する状態となる。そして、暗号化装置１は、ファクシミリ装置３から受信した親展データとパスワードとを送信部６の受信制御部８で読み取り、メモリ部９へ送る。

【００１３】次に、メモリ部９内に送られた親展データとパスワードとのうち、パスワードは、パスワード管理部１０によって、送信した文書を親展機能で受信側の暗号化装置２に処理させるための命令に変換（以下、ヘッダー化という）される。次に、親展データとヘッダー化されたパスワードとは、暗号処理部１１によって、暗号化及び圧縮される（以下、暗号化及び圧縮された親展データとヘッダー化されたパスワードとを一括して送信データという）。そして、送信データは、送信側通信制御部１２によって公衆電話回線５を介して、受信側の暗号化装置２に送信される。このように、ファクシミリ装置３で圧縮した文書を更に圧縮して送信しているので、短時間で大量の文書の送信を行うことが出来る。また、暗号化装置１によって、文書を暗号化して送信しているので、送信の途中で第三者に親展文書を盗まれても、内容を知ることが出来ないので、送信する文書内容の秘密保持を可能にする。

【００１４】次に、親展文書の受信方法について説明する。まず、公衆電話回線５を介して送信された送信データは、受信側の暗号化装置２の受信側通信制御部１３で読み取られ、メモリ部１４へ送られる。そして、メモリ部１４へ送られた送信データは解読処理部１５によって解凍及び解読されて、送信される前の親展データとヘッ

ダー化されたパスワードとに戻され、再びメモリ部１４へ送られる。ここで、メモリ部１４には、送信側の暗号化装置１から送信された状態の送信データ（親展データとヘッダー化されたパスワードとを圧縮及び暗号化したもの）と、解読及び解凍された状態のパスワードと、親展データとが保存されている。次に、メモリ部１４に保存された、ヘッダー化されたパスワードは、パスワード管理部１６によって、パスワードが読み取られる。

【００１５】そして、メモリ部１４内に保存された送信データ（親展データとヘッダー化されたパスワードとを圧縮及び暗号化したもの）と、解凍及び解読された親展文書の送信者情報とが、送受信制御部１７によって受信側のファクシミリ装置４に送信される。そして、送受信制御部１７から送信された、送信者情報と送信データとは、受信側のファクシミリ装置４によって第一回目の印字出力がなされる。ここで、送信者情報と共に印刷される送信データは、受信側の暗号化装置２が受信した状態の送信データ（親展データとヘッダー化されたパスワードとを圧縮及び暗号化したもの）なので、親展文書は暗号化されたままで第一回目の印字出力がなされる。

【００１６】なお、受信側の暗号化装置２が受信した状態の送信データ（親展データとヘッダー化されたパスワードとを圧縮及び暗号化したもの）が大量な場合には、これを全て印字してしまうと、ファクシミリ用紙を無駄に使用してしまう。そこで、受信側の暗号化装置２から受信側のファクシミリ装置４に送信される、受信側の暗号化装置２が受信した状態の送信データを、送信者情報を印刷した部分の下に、送信データの一部（例えば２ｃｍ）だけ印刷するようにすることで、受信された文書が親展文書であることを確認できるようにしている。なお、送信者情報と、受信した状態の送信データとは、同じ紙面上に印刷するようにあらかじめ設定してある。従って、親展文書の特定領域に受取人の宛名及び送信者を特定する情報を記入しておくことで、受取人は、一回の送信によって送信者及び宛先を確認することができる。さらに、送信データの一部が暗号化されたままの状態で出力されるので、たとえ第三者に見られたとしても、送信者は内容の秘密を保持しつつ親展文書を送信することができ、受取人は受信した文書が親展文書であることを容易に確認することが出来る。

【００１７】次に、受信した親展文書を全て出力する第二回目の印字出力方法について説明する。まず、暗号化装置２の受信部７内のメモリ部１４内には、送信データと解読された親展文書が保存されている。ここで、受取人が、受信側のファクシミリ装置４にあらかじめ決めたパスワードを入力する。すると、送受信制御部１７は、ファクシミリ装置４に入力されたパスワードを読み取り、メモリ部１４へ送信する。そして、パスワード管理部１０は、メモリ部１４に保存された、解読及び解凍された状態のパスワードと受信側のファクシミリ装置４に入力されたパスワードとが一致しているかを照合する。ここで、パスワード管理部１０によって、解読及び解凍された状態のパスワードと受信側のファクシミリ装置４に入力されたパスワードとが一致していると確認されると、送受信制御部１７は、メモリ部１４内に保存された、解読及び解凍された親展文書を受信側のファクシミリ装置４に送信する。そして、解読及び解凍された親展文書は、受信側のファクシミリ装置４によって第二回目の印字出力がなされる。このように、受取人があらかじめ決めたパスワードを入力することで、親展文書を印字出力することが出来るようにすることで、受取人のみが親展文書を印字出力することが出来ようになっている。

【００１８】

【発明の効果】以上のように、本発明の暗号化装置は、送信側の通信端末と通信網との間及び受信側の通信端末と通信網との間に設けられ、送信側では通信端末から入力された文書とパスワードとを圧縮し、圧縮された文書とパスワードとを通信網を介して受信側に送信し、受信側では通信網を介して受信した圧縮された文書とパスワードとを解凍し、受信側の通信端末に出力するようにしたことで、ファクシミリ装置で圧縮された文書を更に圧縮するため、通信時間が短縮されるので、通信費を削減することが出来る。

【００１９】また、本発明の暗号化装置は、送信側では圧縮した文書とパスワードとを暗号化し、受信側で圧縮し、暗号化した文書を解読して受信側の通信端末に出力するようにしたことで、送信の途中で第三者に親展文書を盗まれも、親展文書は暗号化されているので、内容を知ることが出来ないので、送信する文書内容の秘密保持を可能にする。

【００２０】また、本発明の暗号化装置は、受信側において、通信網を介して受信した圧縮し、暗号化した文書を解凍及び解読し、解凍及び解読された文書の特定領域と、通信網を介して受信した圧縮し、暗号化した文書とを受信側の通信端末に出力するようにしたことで、例えば、受取人の宛名及び送信者の特定する情報を特定領域に記載することによって、、あらかじめ親展文書を送る旨の通知をすることなく親展文書の送受信を行うことができる。

【００２１】また、本発明の暗号化装置は、受信側において、圧縮し暗号化された文書とパスワードとを受信したときに、受信側の通信端末に入力されたパスワードによって、解読した文書を出力するようにしたことで、パスワードを知っている受取人のみが解凍及び解読された親展文書を印字出力することを可能にする。

【図面の簡単な説明】

【図１】本発明の暗号化装置を用いた親展文書の送受信の概略の図である。

【図２】本発明の暗号化装置のブロック図である。

【図３】従来のファクシミリ装置を用いた親展文書送信

の実施例である。

【符号の説明】

１，２　暗号化装置

３，４　ファクシミリ装置

５　公衆電話回線

６　送信部

７　受信部

８　受信制御部

９，１４　メモリ部

１０，１６　パスワード管理部

１１　暗号処理部

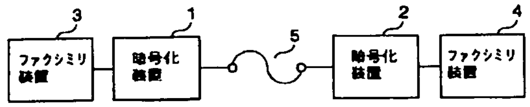
１２　送信側通信制御部

１３　受信側通信制御部

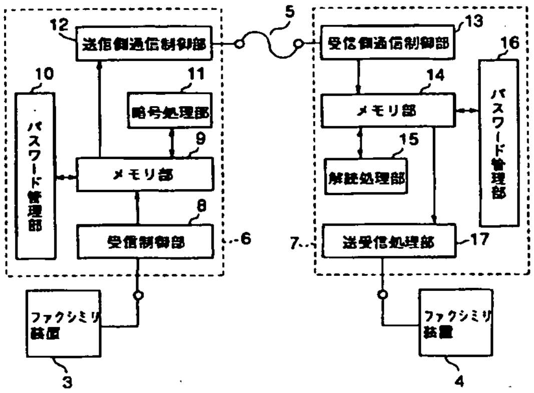
１５　解読処理部

１７　送受信制御部

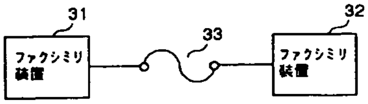
【図１】



【図２】



【図３】


31
ファクシミリ装置
33
32
ファクシミリ装置